
Department: UW Medicine Information Technology Services

Policy Number: SEC-01.01 Management of Information Security Policies, Standards, Guidelines, and Procedures

Effective Date: June 11th, 2007

Review Date: April 27th, 2007

Purpose

This standard specifies the requirements for development, approval, review, and revision of UW Medicine Information Security policies, standards, guidelines, and procedures.

Definitions

See UW Medicine Information Security policy: *SEC-REF UW Medicine Information Security Program Glossary of Terms*.

Policy

UW Medicine creates and maintains Information Security policies, standards, guidelines, and procedures as required to meet compliance, risk management, operational, and financial objectives. Drafting and approval of these documents follows a defined process, with clear roles and responsibilities assigned. Policies, standards, guidelines, and procedures will be reviewed and revised in a timely manner as the UW Medicine operating environment changes and technology advances.

I. Document Development and Approval

A. Policies and Standards

The security director in coordination with CASC will lead the drafting, editing, or revision of UW Medicine policies, procedures, guidelines and standards. CASC may also request review by one or all of the following entities:

- Confidentiality and Access Working Group (CAWG)
- Security Implementation Oversight Group (SIOG)
- Attorney General's Office (AGO)
- PASS Council
- HIPPA Program Office

- Others entities as CASC deems necessary

II. Document Review and Revision

Policies, Standards, Guidelines, and Procedures

- A. UW Medicine Information Security policies and standards are reviewed by CASC at least every three years. Reviews at shorter intervals may be triggered by changes to state and federal laws, significant changes within the UW Medicine operating environment, the outcome of risk assessments, or by the development of enabling technologies.
- B. When a review indicates that changes are required to an approved UW Medicine policy, standard, guideline, or procedure, the document will be revised. The revision and approval process follows the same course as that for new policies, standards, guidelines, and procedures (see section above).

III. Document Retention

Records of the drafting, approval, revision, and exemption processes will be maintained for no less than 6 years.

IV. Departmental and System-Specific Policies, Standards, Guidelines, and Procedures

Departmental administrators, system owners, and data custodians may create departmental or system-specific policies and standards to meet their special needs. These policies and standards should be developed when more stringent requirements are warranted or when a departmental or system specific policy need is not addressed by UW Medicine policy. They may not be less stringent than UW Medicine policies and standards. Department administrators and/or System Owners may develop or update their own guidelines and procedures to ensure that their operations and systems remain or become compliant with UW Medicine policies and standards.

Review and revision of departmental and system-specific policies, standards, guidelines, and procedures is the responsibility of the respective departmental administrator, system owner, or data custodian. Departmental and system specific policies and standards must be reviewed at least every three years.

References:

- I. 45 CFR Part 164; Section 164.308(a)(1) (i) Security Management Process
- II. 45 CFR Part 164; Section 164.308(a)(2) Assigned Security Responsibility

- III. 45 CFR Part 164; Section 164.316 Policies and Procedures and Documentation Requirements
- IV. International Organization for Standardization /International Electrotechnical Commission (ISO/IEC) 17799 Section 3, Security Policy

UW Medicine IT Services: _____ Date: _____

James S. Fine, M.D., CIO, ISO
